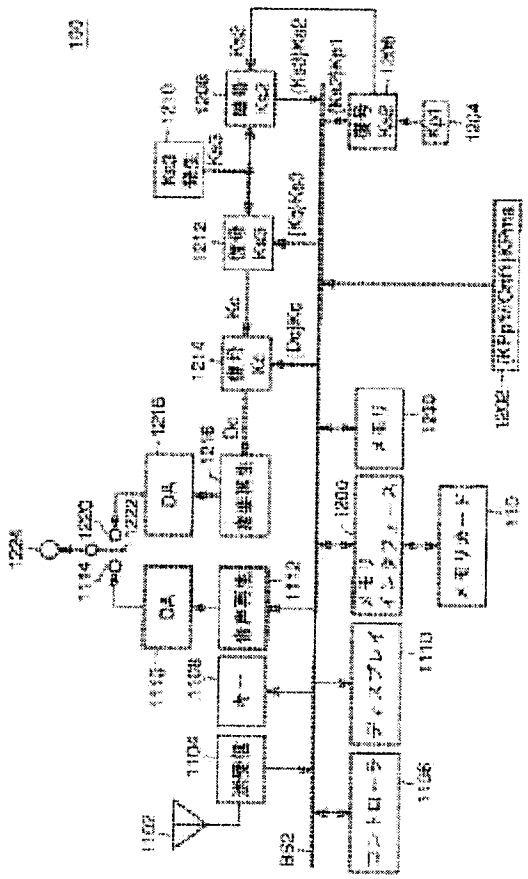
DATA REPRODUCING DEVICE AND LICENSE MANAGING METHOD

Publication number: JP2002099743 (A)
Publication date: 2002-04-05
Inventor(s): MORIAI SHINSUKE
Applicant(s): SANYO ELECTRIC CO
Classification:
- international: ***G06Q30/00; G06Q10/00; G06Q50/00; G09C1/00; G10K15/02;*** **G06Q30/00; G06Q10/00; G06Q50/00; G09C1/00; G10K15/02;** (IPC1-7): G06F17/60; G09C1/00
- European:
Application number: JP20000287909 20000922
Priority number(s): JP20000287909 20000922

Abstract of **JP 2002099743 (A)**

PROBLEM TO BE SOLVED: To provide a data reproducing device and a license managing method with a procedure where the selection of music and the management of contents are simplified. SOLUTION: A portable telephone set 100 includes a controller 1106, a display 1110, a key operation part 1108, a memory 1230, a memory card 110 and a reproduction system circuit. In a music reproducing mode, information (reproduced music list) on reproducible contents data is displayed on the display 1110 based on an inter-media music list recorded in the memory card 110. A user selects music from pertinent display. In a media managing mode, compiling work is possible corresponding to the inter-media music list showing the data contents recorded in the memory card 110.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－99743
（P2002－99743A）
(43)公開日　平成14年４月５日(2002.4.5)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ	５Ｂ０４９
	１３２		１３２	５Ｊ１０４
	１４２		１４２	
	５０６		５０６	
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	

審査請求　未請求　請求項の数13　ＯＬ　（全 23 頁）

(21)出願番号　特願2000－287909(P2000－287909)

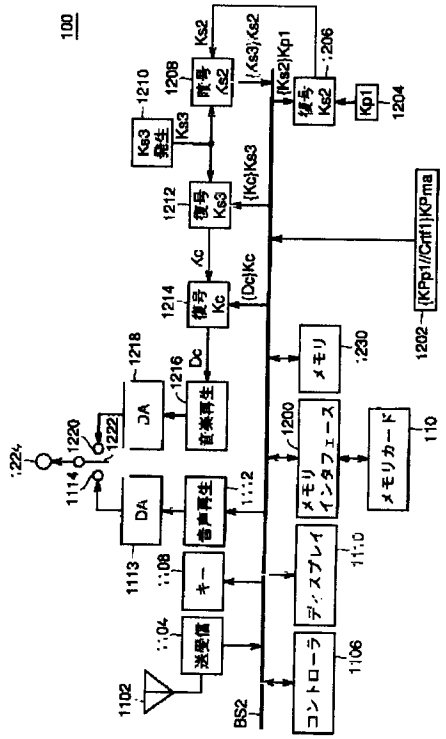
(22)出願日　平成12年９月22日(2000.9.22)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　盛合　真介
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

Ｆターム(参考)　5B049 AA02 AA05 CC09 DD01 EE05
FF07 GG03 GG04 GC07
5J104 AA01 AA16 EA04 EA15 NA02
NA37 PA02 PA07 PA14

(54)【発明の名称】　データ再生装置およびライセンス管理方法

(57)【要約】
【課題】　選曲およびコンテンツの管理が簡単化した手続きで実現可能なデータ再生装置およびライセンス管理方法を提供する。
【解決手段】　携帯電話機１００は、コントローラ１１０６、ディスプレイ１１１０、キー操作部１１０８、メモリ１２３０、メモリカード１１０および再生系回路を含む。音楽再生モードでは、メモリカード１１０に記録されるメディア内曲リストに基づき、再生可能なコンテンツデータの情報（再生曲リスト）をディスプレイ１１１０に表示する。ユーザは、当該表示から選曲する。メディア管理モードでは、メモリカード１１０に記録されるデータ内容を示すメディア内曲リストに対し、編集作業を可能とする。



【特許請求の範囲】
【請求項１】　コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、前記データ記録装置に記録された前記暗号化コンテンツデータを再生するデータ再生装置であって、
外部との通信を行なう通信部と、
データ授受を制御するインタフェースと、
制御部と、
表示部とを備え、
前記制御部は、
前記再生時に、再生可能な前記暗号化コンテンツデータに関するコンテンツリストを前記表示部に表示する、データ再生装置。
【請求項２】　前記コンテンツリストのなかから再生する前記暗号化コンテンツデータが選択される、請求項１に記載のデータ再生装置。
【請求項３】　前記制御部は、
前記データ記録装置に記録されるデータに基づき、コンテンツ毎に、前記暗号化コンテンツデータおよび前記ライセンス情報、前記暗号化コンテンツデータのみ、または前記ライセンス情報のみが存在することを示す情報を含むメディア内コンテンツリストを生成し、前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項１に記載のデータ再生装置。
【請求項４】　前記データ記録装置は、
記録されるデータに基づき、コンテンツ毎に、前記暗号化コンテンツデータおよび前記ライセンス情報、前記暗号化コンテンツデータのみ、または前記ライセンス情報のみが存在することを示す情報を含むメディア内コンテンツリストを生成し、
前記制御部は、
前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項１に記載のデータ再生装置。
【請求項５】　前記制御部は、
前記データ記録装置に記録されるデータに基づき、コンテンツ毎に、前記ライセンス情報により再生に制限があるか否かを示す情報を含むメディア内コンテンツリストを生成し、前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項１に記載のデータ再生装置。
【請求項６】　前記データ記録装置は、
記録されるデータに基づき、コンテンツ毎に、前記ライセンス情報により再生に制限があるか否かを示す情報を含むメディア内コンテンツリストを生成し、
前記制御部は、
前記再生時において、前記メディア内コンテンツリストに基づき、前記コンテンツリストを生成する、請求項１に記載のデータ再生装置
【請求項７】　前記制御部は、
前記暗号化コンテンツデータおよび前記ライセンス情報の双方が存在するコンテンツに関する情報を表示する、請求項１に記載のデータ再生装置。
【請求項８】　前記制御部は、
前記再生時において、前記ライセンス情報に基づき再生不可能になった前記暗号化コンテンツデータに関する情報については、前記コンテンツリストから削除する、請求項１から７のいずれか１項に記載のデータ再生装置。
【請求項９】　前記制御部は、メディア管理モードでは、前記メディア内コンテンツリストを前記表示部に表示し、
前記表示部に表示される前記メディア内コンテンツリストにおいて変更可能なデータを編集するための回路をさらに備える、請求項３、４、５、６のいずれか１項に記載のデータ再生装置
【請求項１０】　コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、前記データ記録装置に記録された前記暗号化コンテンツデータを再生するデータ再生装置におけるライセンス管理方法であって、
モードを判定するステップと、
前記判定により再生モードであると判定される場合に、再生可能な前記暗号化コンテンツデータに関するコンテンツリストを生成するステップと、前記コンテンツリストを表示する表示ステップとを含む再生ステップと備える、ライセンス管理方法。
【請求項１１】　前記再生ステップは、
前記再生時において、前記ライセンス情報に基づき再生不可能になった前記暗号化コンテンツデータについては、前記コンテンツリストから削除するステップを含む、請求項１０に記載のライセンス管理方法。
【請求項１２】　前記データ記録装置に記録されるデータに基づき、メディア内コンテンツリストを生成するステップをさらに備え、
前記コンテンツリストは、前記メディア内コンテンツリストに基づき生成される、請求項１０に記載のライセンス管理方法。
【請求項１３】　前記モードを判定するステップにおいてメディア管理モードであると判定される場合に、前記メディア内コンテンツリストにおいて変更可能なデータを編集することができるステップをさらに備える、請求項１２に記載のライセンス管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ再生装置およびライセンス管

理方法に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００６】

【発明が解決しようとする課題】ところで、コンテンツデータを再生するための復号鍵（ライセンス）には、再生回数制限や期日制限などを設定することができる。

【０００７】しかし、著作権保護が必要とされるコンテンツデータを復号する（再生する）場合に、ユーザがその都度ライセンス状態を確認する必要があるとすれば、ユーザ側にとって再生手続きが煩雑になる。

【０００８】また、ユーザ側は、このようなダウンロードしたコンテンツデータを簡単な手続きで管理したいという要望もある。

【０００９】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、再生モードにおいて、自動的にライセンス状態を判別して再生可能な暗号化コンテンツデータを提示することができるデータ再生装置およびライセンス管理方法を提供することである。

【００１０】また、さらなる目的は、ダウンロードした暗号化コンテンツデータを簡単な手続きで管理することができるデータ再生装置およびライセンス管理方法を提供することである。

【００１１】

【課題を解決するための手段および発明の効果】この発明のある局面によるデータ再生装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、データ記録装置に記録された暗号化コンテンツデータを再生するデータ再生装置であって、外部との通信を行なう通信部と、データ授受を制御するインタフェースと、制御部と、表示部とを備える。制御部は、再生時に、再生可能な暗号化コンテンツデータに関するコンテンツリストを表示部に表示する。

【００１２】好ましくは、コンテンツリストのなかから再生される暗号化コンテンツデータが選択される。

【００１３】好ましくは、制御部は、データ記録装置に記録されるデータに基づき、メディア内コンテンツリストを生成し、再生時において、メディア内コンテンツリストに基づき、コンテンツリストを生成する。

【００１４】好ましくは、データ記録装置は、記録されるデータに関する情報を含むメディア内コンテンツリストを生成し、制御部は、再生時において、メディア内コンテンツリストに基づき、コンテンツリストを生成する。

【００１５】メディア内コンテンツリストは、コンテンツ毎に、暗号化コンテンツデータおよびライセンス情報、暗号化コンテンツデータのみ、またはライセンス情報のみが存在することを明示する情報を含む。また、メディア内コンテンツリストは、コンテンツ毎に、ライセンス情報により再生に制限があるか否かを示す情報を含む。

【００１６】特に、制御部は、暗号化コンテンツデータおよびライセンス情報の双方が存在するコンテンツに関する情報を表示する。

【００１７】特に、制御部は、再生時において、ライセンス情報に基づき再生不可能になった暗号化コンテンツデータについては、コンテンツリストから削除する。

【００１８】特に、制御部は、メディア管理モードでは、メディア内コンテンツリストを表示部に表示し、表示部に表示されるメディア内コンテンツリストにおいて変更可能なデータを編集するための回路をさらに備える。

【００１９】この発明のさらなる局面によるライセンス管理方法は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータに関するライセンス情報とをダウンロードしてデータ記録装置に記録し、データ記録装置に記録された暗号化コンテンツデータを再生するデータ再生装置におけるライセンス管理方法であって、モードを判定するステップと、判定により再生モードであると判定される場合に、再生可能な暗号化コンテンツデータに関するコンテンツリストを生成するステップと、コンテンツリストを表示する表示ステップとを含む再生ステップと備える。

【００２０】好ましくは、再生ステップは、再生時に，ライセンス情報に基づき再生不可能になった暗号化コンテンツデータについては、コンテンツリストから削除するステップをさらに含む。

【００２１】好ましくは、データ記録装置に記録されるデータに基づき、メディア内コンテンツリストを生成す

るステップをさらに備え、コンテンツリストは、メディア内コンテンツリストに基づき生成される。

【００２２】特に、モードを判定するステップにおいて、メディア管理モードであると判定される場合に、メディア内コンテンツリストにおいて変更可能なデータを編集することができるステップをさらに備える。

【００２３】したがって、この発明によれば、再生側において、ライセンスの制限を自動的に判別できるため、ユーザ側の選曲動作が簡単化される。また、コンテンツに関する変更可能なデータをユーザ側で編集することができるため、ユーザ側の意向にそったデータ管理が可能になる。

【００２４】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００２５】［第１の実施の形態］図１は、本発明によるデータ端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００２６】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。また、他の情報通信網を介して配信する場合においても適用可能である。

【００２７】図１を参照して、著作権の存在する音楽データを管理するライセンスサーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザ１の携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータを与える。

【００２８】配信キャリア２０は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ１０に中継する。ライセンスサーバ１０は、配信リクエストがあると、メモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア２０の携帯電話網を介して、各携帯電話ユーザの携帯電話機を介して装着されたメモリカードに対してコンテンツデータを配信する。

【００２９】図１においては、たとえば携帯電話ユーザ１の携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、格納する。また、上記配信にあたって行なわれた認証処理によりライセンスキーを受取り、データを格納する。暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００３０】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホン１３０等を介してライセンスキーにより暗号化コンテンツデータを復号して「再生」し、聴取することが可能である。

【００３１】以下では、このようなライセンスサーバ１０と配信キャリア２０と併せて、配信サーバ３０と総称することにする。

【００３２】また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００３３】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００３４】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００３５】このような構成において、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号化鍵を配信するための方式である。第２には、配信したいコンテンツデータを暗号化する方式そのものである。第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００３６】そして、第４には、再生モードにおいて、ライセンス状態を自動的に判別するための構成である。さらに、第５には、コンテンツに関するリストをユーザが編集可能とするための構成である。

【００３７】第１の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生装置（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成、ならびにコンテンツデータに関するリストをユーザに提示するとともに、ユーザ側で当該リストの編集を行える構成を示す。

【００３８】図２は、図１に示したデータ配信システム

において、使用される通信のためのデータ、情報等の特性を説明する図である。

【００３９】まず、配信サーバ３０より配信されるデータについて説明する。Ｄａｔａは、音楽データ等のコンテンツデータである。コンテンツデータＤａｔａには、ライセンスキーＫｃで復号可能な暗号化が施される。ライセンスキー（「コンテンツ鍵」とも言う。以下同じ。）Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

【００４０】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００４１】さらに、配信サーバ３０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、ライセンス情報としては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１および再生回路における制御情報である再生回路制御情報ＡＣ２等が存在する。以後、ライセンスキーＫｃとコンテンツＩＤとライセンスＩＤとアクセス制御情報ＡＣ１と再生回路制御情報ＡＣ２とを併せて、ライセンスと総称することとする。

【００４２】図3は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【００４３】第１の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生するデータ端末装置（携帯電話機）のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００４４】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止されるデータ端末装置およびメモリカードのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。

【００４５】禁止クラスリストデータＣＲＬは、配信サーバ３０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データＣＲＬ＿ｄａｔを配信サーバ３０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬが書替えられる構成とする。また、禁止クラスリストのバージョンについては、ＣＲＬ＿ｖｅｒをメモリカード側より出力し、これを配信サーバ３０側で確認することによってバージョン管理を実行する。差分データＣＲＬ＿ｄａｔには新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【００４６】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、データ端末装置およびメモリカードの種類に固有の復号鍵が破られた、データ端末装置およびメモリカードへのライセンスキーの供給を禁止する。このため、データ端末装置ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【００４７】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【００４８】データ端末装置およびメモリカードには固有の公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉがそれぞれ設けられ、公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉはデータ端末装置に固有の秘密復号鍵Ｋｐｎおよびメモリカード固有の秘密復号鍵Ｋｍｃｉによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、データ端末装置の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【００４９】また、再生回路およびメモリカードのクラス証明書として、ＣｒｔｆｎおよびＣｍｃｉがそれぞれ設けられる。

【００５０】これらのクラス証明書は、メモリカードおよびコンテンツ再生部（携帯電話機）のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【００５１】これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａおよび｛ＫＰｐｎ／／Ｃｒｔｆｎ｝ＫＰｍａの形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。後ほど

詳細に説明するが、ＫＰｍａは配信システム全体で共通の公開認証鍵である。

【００５２】図4は、図1に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【００５３】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ３０、携帯電話機１００、メモリカード１１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００５４】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００５５】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００５６】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍと、公開暗号鍵ＫＰｍで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍが存在する。

【００５７】図5は、図1に示したライセンスサーバ１０の構成を示す概略ブロック図である。

【００５８】ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４、課金データベース３０２およびＣＲＬデータベース３０６からのデータをデータバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００５９】データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを通信装置３５０およびデータバスＢＳ１を介して受けて、公開認証鍵ＫＰｍａによる復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｉを用いて暗号化して、データバスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをデータバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００６０】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンスキーＫｃおよび再生回路制御情報ＡＣ２を、復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してデータバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【００６１】ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００６２】図6は、図1に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【００６３】携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

【００６４】携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのキー操作部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを含む。

【００６５】携帯電話機１００は、さらに、音声再生部１１１２の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１１１３と、ＤＡ変換器１１１３の出力を外部出力装置等へ出力するための端子１１１４とを含む。

【００６６】携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００とを含む。

【００６７】携帯電話機１００は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｒｔｆ１を公開復号鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを保持する認証データ保持部１２０２を含む。

【００６８】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１２０４と、データバスＢＳ２から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１２０６とを含む。

【００６９】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でデータバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１２１０と、生成されたセッションキーＫｓ３を復号処理部１２０６によって得られたセッションキーＫｓ２によって暗号化しデータバスＢＳ２に出力する暗号化処理部１２０８とを含む。

【００７０】携帯電話機１００は、さらに、データバスＢＳ２上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１２１２とを含む。

【００７１】携帯電話機１００は、さらに、データバスＢＳ２より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１２１２より取得したライセンスキーＫｃによって復号しコンテンツデータを出力する復号処理部１２１４と、復号処理部１２１４の出力を受けてコンテンツデータを再生するための音楽再生部１２１６と、音楽再生部１２１６の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１２１８と、ＤＡ変換器１１１３とＤＡ変換器１２１８との出力を受けて、動作モードに応じて選択的に端子１１１４または端子１２２０から出力するためのスイッチ１２２２と、スイッチ１２２２の出力を受けて、ヘッドホーン１３０と接続するための接続端子１２２４と、データを記録するメモリ１２３０とを含む。

【００７２】コントローラ１１０６は、データダウンロード処理、データの再生処理、電源制御処理等を行うとともに、再生曲リストの生成、メディア管理モードでのメディア曲リストの生成、表示制御等を行う。

【００７３】なお、図６においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【００７４】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００７５】図7は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃｉおよびＫｍｃｉが設けられ、メモリカードのクラス証明書Ｃｍｃｉが設けられるが、メモリカード１１０においては、これらは自然数ｉ＝１でそれぞれ表わされるものとする。

【００７６】したがって、メモリカード１１０は、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ１を保持するＫｍｃ保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Ｋｍ１を保持するＫｍ１保持部１４２１と、Ｋｍ１によって復号可能な公開暗号鍵ＫＰｍ１を保持するＫＰｍ１保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される公開暗号鍵ＫＰｍｃ１およびクラス証明書Ｃｍｃ１を公開認証鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａとして保持する。

【００７７】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

【００７８】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０１を介して授受するデータバスＢＳ３と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Ｋｍｃ１をＫｍｃ１保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ１を接点Ｐａに出力する復号処理部１４０４と、ＫＰｍａ保持部１４１４から認証鍵ＫＰｍａを受けて、データバスＢＳ３に与えられるデータからＫＰｍａによる復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してデータバスＢＳ３に出力する暗号化処理部１４０６とを含む。

【００７９】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２

を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｎもしくはＫＰｍｃｉによって暗号化してデータバスＢＳ３に送出する暗号化処理部１４１０と、データバスＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号し、復号結果をデータバスＢＳ４に送出する復号処理部１４１２とを含む。

【００８０】メモリカード１１０は、さらに、データバスＢＳ３上のデータを公開暗号鍵ＫＰｍ１と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号するための復号処理部１４２２と、公開暗号鍵ＫＰｍ１で暗号化されている、ライセンスキーＫｃ、再生回路制御情報ＡＣ２および再生情報（コンテンツＩＤ，ライセンスＩＤ，アクセス制御情報ＡＣ１）と、暗号化されていない禁止クラスリストのバージョン更新のための差分データＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬとをデータバスＢＳ４より受けて格納するとともに、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。

【００８１】メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を保持するためのライセンス情報保持部１４４０と、データバスＢＳ３を介して外部との間でデータ授受を行ない、データバスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【００８２】ライセンス情報保持部１４４０は、データバスＢＳ４との間でライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１のデータの授受が可能である。ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

【００８３】なお、図７において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）である。

【００８４】もちろん、メモリ１４１５も含めて、モジュールＴＲＭ内に組込まれる構成としてもよい。しかしながら、図７に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

【００８５】次に、図１に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【００８６】図８および図９は、図１に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１および第２のフローチャートである。

【００８７】図８および図９においては、携帯電話ユーザ１が、メモリカード１１０を用いることで、携帯電話機１００を介して配信サーバ３０から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【００８８】まず、携帯電話ユーザ１の携帯電話機１００から、携帯電話ユーザ１によるキー操作部１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【００８９】メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａが出力される（ステップＳ１０２）。

【００９０】携帯電話機１００は、メモリカード１１０からの認証のための認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

【００９１】配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａ、ライセンス購入条件データＡＣを受信し（ステップＳ１０６）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰｍａで復号処理を実行する（ステップＳ１０８）。

【００９２】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍｃ１と証明書Ｃｍｃ１を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１０）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を承認し、受理する。そして、次の処理（ステップＳ１１２）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を受理しないで処理を終了する（ステップＳ１７

０）。

【００９３】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍｃ１が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

【００９４】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

【００９５】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ１によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

【００９６】暗号化されたセッションキーＫｓ１は、｛Ｋｓ１｝Ｋｍｃ１として、データバスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

【００９７】携帯電話機１００が、暗号化されたセッションキー｛Ｋｓ１｝Ｋｍｃ１を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ１により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１２０）。

【００９８】コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

【００９９】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストの状態（バージョン）に関連する情報として、リストのバージョンデータＣＲＬ＿ｖｅｒをメモリ１４１５から抽出してデータバスＢＳ４に出力する。

【０１００】暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍ１および禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１をデータバスＢＳ３に出力する（ステップＳ１２２）。

【０１０１】データバスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１は、データバスＢＳ３から端子１２０１およびメモリインタフェース１２００を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

【０１０２】配信サーバ３０は、暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍ１およびメモリカード１１０における禁止クラスリストのバージョンデータＣＲＬ＿ｖｅｒを受理する（ステップＳ１２６）。

【０１０３】禁止クラスリストのバージョン情報ＣＲＬ＿ｖｅｒは、データバスＢＳ１を介して配信制御部３１５に送られ、配信制御部３１５は、受理したバージョンデータＣＲＬ＿ｖｅｒに従って、当該ＣＲＬ＿ｖｅｒのバージョンとＣＲＬデータベース３０６内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データＣＲＬ＿ｄａｔを生成する（ステップＳ１２８）。

【０１０４】さらに、配信制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件データＡＣに従って、ライセンスＩＤ、アクセス制限情報ＡＣ１および再生回路制御情報ＡＣ２を生成する（ステップＳ１３０）。さらに、暗号化コンテンツデータを復号するためのライセンスキーＫｃを情報データベース３０４より取得する（ステップＳ１３２）。

【０１０５】図９を参照して、配信制御部３１５は、生成したライセンス、すなわち、ライセンスキーＫｃ、再生回路制御情報ＡＣ２、ライセンスＩＤ、コンテンツＩＤ、およびアクセス制限情報ＡＣ１を暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ１によってライセンスを暗号化する（ステップＳ１３６）。暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がデータバスＢＳ１を介して供給する禁止クラスリストの差分データＣＲＬ＿ｄａｔとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、データバスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

【０１０６】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗

号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0107】携帯電話機100は、送信された暗号化データ｛｛Kc//AC2//ライセンスID//コンテンツID//AC1｝Km1//CRL_dat｝Ks2を受信し（ステップS140）、メモリインタフェース1200を介してメモリカード110へ出力する。メモリカード110においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてデータバスBS3の受信データを復号しデータバスBS4に出力する（ステップS142）。

【0108】この段階で、データバスBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス｛Kc//AC2//ライセンスID//コンテンツID//AC1｝Km1と、CRL_datとが出力される。コントローラ1420の指示によって、暗号化ライセンス｛Kc//AC2//ライセンスID//コンテンツID//AC1｝Km1は、メモリ1415に記録される（ステップS144）。一方、暗号化ライセンス｛Kc//AC2//ライセンスID//コンテンツID//AC1｝Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンスのうち、メモリカード110内で参照されるライセンスID、コンテンツIDおよびアクセス制限情報AC1のみが受理される（ステップS146）。

【0109】コントローラ1420は、受理したCRL_datに基づいて、メモリ1415内の禁止クラスリストデータCRLおよびそのバージョンを更新する（ステップS148）。さらに、ライセンスID、コンテンツIDおよびアクセス制限情報AC1については、ライセンス情報保持部1440に記録される（ステップS150）。

【0110】ステップS150までの処理がメモリ回路で正常に終了した段階で、携帯電話機100から配信サーバ30にコンテンツデータの配信要求がなされる（ステップS152）。

【0111】配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data－infを取得して、これらのデータをデータバスBS1および通信装置350を介して出力する（ステップS154）。

【0112】携帯電話機100は、｛Data｝Kc//Data－infを受信して、暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data－infを受理する（ステップS156）。暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data－infは、メモリインタフェース1200および端子1201を介してメモリカード110のデータバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data－infがそのままメモリ1415に記録される（ステップS158）。

【0113】さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され（ステップS160）、配信サーバ30で配信受理を受信すると（ステップS162）、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され（ステップS164）、全体の処理が終了する（ステップS170）。

【0114】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信できた公開暗号鍵KPp1およびKPmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵KPp1およびKPmc1による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0115】次に、メモリカード110に配信されたコンテンツデータの携帯電話機100における音楽再生に関する処理について、図10を用いて説明する。

【0116】メモリカード110は、メディア内にある曲データおよびライセンス情報をメモリ1415に記録している。携帯電話機100は、メモリカード内110の曲情報を取出し、メディア内曲リストR1として生成し、メモリ1230に記録する。

【0117】メディア内曲リストR1は、暗号化コンテンツデータ｛Data｝Kcとともに配信サーバ30から送信されるメタデータから曲名等の主要な関連情報を抽出して作成されたものである。

【0118】メディア内曲リストR1は、図10（a）に示すように、記録される各曲データの特性を示す特性リスト500と、記録される各曲データの曲名とアーティスト名とを示す曲名・アーティスト名リスト501とから成る。

【0119】図においては、特性リスト500には、再生番号001～006，“L”，“C”が記録され、曲名・アーティスト名リスト501には、曲名1～11と対応するアーティスト名A～Fとが記録されている。

【0120】特性リスト500の再生番号は、再生可能な曲データに割当てられた番号である。

【0121】特性リスト500に、“L”が記録されて

いる曲は、メモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃだけが存在しライセンスキーＫｃがないことを示す。たとえば、携帯電話機のユーザ１が、パソコンや他の携帯電話機のユーザ２等から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをコピーしたり、ダウンロードした場合がこれに相当する。

【０１２２】特性リスト５００に、“Ｃ”が記録されている曲は、メモリカード１１０にライセンスキーＫｃは存在するが暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃが存在しないことを示す。たとえば、ユーザ１がメモリカード１１０内にライセンスキーと暗号化コンテンツデータとを持っていた状態で、パソコン等などを用いて他の記録媒体に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを移動することで、メモリカード１１０から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃが削除された場合がこれに相当する。また、携帯電話機のユーザ２が、携帯電話機のユーザ１から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受け、ユーザ１の携帯電話機から当該暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃが削除された場合もこれに相当する。

【０１２３】携帯電話機１００は、コントローラ１１０６の制御に基づき、再生モード時に再生曲リストＲ２を生成する。再生曲リストＲ２は、メモリ１２３０に記録される。再生曲リストＲ２は、図１０（ｂ）に示すように、再生番号を示す再生番号リスト５１０と、曲名・アーティスト名リスト５１１とから成る。

【０１２４】再生曲リストＲ２は、メディア内曲リストＲ１に記録される曲データのうちコンテンツデータとライセンスデータとが揃った再生可能な曲データを抽出して作成される。より具体的には、再生曲リストＲ２は、再生番号を有する曲データに基づき生成される。

【０１２５】再生曲リストＲ２は、たとえば、携帯電話機１００のディスプレイ１１１０に表示される。ユーザは、表示される再生曲リストＲ２のなかから再生する曲を選曲する。

【０１２６】第１の実施の形態では、ライセンスによる制限に基づき、メディア内曲リストＲ１が更新される。そして、メディア内曲リストＲ１に従って再生曲リストＲ２が更新される。

【０１２７】たとえば、図１１（ａ）に示す再生番号００４の曲名８／アーティストＤについて、ライセンスが再生期日の制限がついていた場合、ライセンスで指定される再生期日が過ぎた時には、図１１（ｂ）に示すように再生番号００４が特性“ＬＮ”に変わる。また、ライセンスで制限されるのが再生回数であった場合、ライセンスにより再生回数が制限値に到達した時にも、再生番号が、ライセンス制限により再生できないことを示す記号（たとえば、“ＬＣ”）に変わる。

【０１２８】たとえば、図１２（ａ）に示すように、再生曲リストＲ２のうち再生番号００１～００６が付される曲名１，３，４，８，１０，１１から選曲を行うとする。再生番号００４に再生回数制限があるとする。再生番号００４が、再生回数分だけ再生された場合、図１２（ｂ）に示すように再生番号００４が再生曲リストから削除される。そして、図１２（ｃ）に示すように再生番号が自動的に修正され、曲名１，３，８，１１に対して再生番号００１，００２，００３，００４，００５が割当てられる。

【０１２９】次に、携帯電話機１００におけるコンテンツデータの再生動作の流れについて説明する。

【０１３０】図１３を参照して、初期状態として待ち受け状態にあるとする。音楽再生モードに入ると（ステップＳ２００）、コントローラ１１０６は、データバスＢＳ２を介して認証データ保持部１２０２から認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを読出し、メモリインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを入力する（ステップＳ２０１）。

【０１３１】メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを受理する（ステップＳ２０２）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを、ＫＰｍａ保持部１４１４に保持された公開認証鍵ＫＰｍａによって復号し（ステップＳ２０３）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ２０４）。

【０１３２】認証データが復号できなかった場合、コントローラ１４２０は認証データ不受理の出力をデータバスＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２３０）。そして再生不能の表示を行い（ステップＳ２３１）、音楽再生モードを終了する。

【０１３３】認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｒｔｆ１がメモリ１４１５から読出した禁止クラスリストデータに含まれるか否かを判断する（ステップＳ２０５）。この場合、証明書Ｃｒｔｆ１にはＩＤが付与されており、コントローラ１４２０は、受理した証明書Ｃｒｔｆ１のＩＤが禁止クラスリストデータの中に存在するか否かを判別する。証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれると判断されると、コントローラ１４２０は認証データ不受理の出力をデータバスＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２３０）。

【０１３４】ステップＳ２０４において認証データが公開認証鍵ＫＰｍａで復号できなかったとき、およびステップＳ２０５において受理した証明書Ｃｒｔｆ１が禁止

クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機１００のコントローラ１１０６は、認証データ不受理のため再生不可能であることをディスプレイ１１１０に表示する。

【０１３５】ステップＳ２０５において、証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれていないと判断されると、再生曲リストＲ２が生成され、表示される（ステップＳ２０６）。再生曲リストＲ２が表示されると、ユーザによる選曲モードになる（ステップＳ２０７）。

【０１３６】選曲されると、図１４を参照して、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ２０８）。そして、暗号化処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をデータバスＢＳ３へ出力する（ステップＳ２０９）。そうすると、コントローラ１４２０は、端子１２０１を介してメモリインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力し、携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１２０４は、秘密復号鍵Ｋｐ１を復号処理部１２０６へ出力する。

【０１３７】復号処理部１２０６は、Ｋｐ１保持部１２０４から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号化処理部１２０８へ出力する（ステップＳ２１０）。そうすると、セッションキー発生部１２１０は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号化処理部１２０８へ出力する（ステップＳ２１１）。暗号化処理部１２０８は、セッションキー発生部１２１０からのセッションキーＫｓ３を復号処理部１２０６からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、データバスＢＳ２およびメモリインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ２１２）。

【０１３８】メモリカード１１０の復号処理部１４１２は、端子１２０１およびデータバスＢＳ３を介して｛Ｋｓ３｝Ｋｓ２を入力し、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、携帯電話機１００で発生されたセッションキーＫｓ３を取得する（ステップＳ２１３）。

【０１３９】セッションキーＫｓ３の受理に応じて、コントローラ１４２０は、ライセンス情報保持部１４４０内の対応するアクセス制限情報ＡＣ１を確認する（ステップＳ２１４）。

【０１４０】ステップＳ２１４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１を確認する。再生不可の状態である場合には再生動作を終了し、再生回数に制限がある場合にはアクセス制限情報ＡＣ１のデータを更新し再生可能回数を更新する。そして、次のステップに進む（ステップＳ２１５）。アクセス制限情報ＡＣ１が更新されると、携帯電話機１００側においてもメディア内曲リストＲ１も更新される。

【０１４１】アクセス制限情報ＡＣ１によって再生回数が制限されていない場合においては、ステップＳ２１５はスキップされ、アクセス制限情報ＡＣ１は更新されることなく次の処理に進む（ステップＳ２１６）。

【０１４２】ステップＳ２１４において、当該再生動作において再生が可能であると判断された場合には、選曲された曲データのライセンスキーＫｃを含むライセンスの復号処理が実行される。具体的には、コントローラ１４２０の指示に応じて、メモリ１４１５からデータバスＢＳ４に読出された暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１を復号処理部１４２２がメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号し、再生処理に必要なライセンスキーＫｃと再生回路制御情報ＡＣ２がデータバスＢＳ４上に得られる（ステップＳ２１６）。

【０１４３】得られたライセンスキーＫｃと再生回路制御情報ＡＣ２は、切換スイッチ１４４４の接点Ｐｄを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｄを介して復号処理部１４１２より受けたセッションキーＫｓ３によってデータバスＢＳ４から受けたライセンスキーＫｃと再生回路制御情報ＡＣ２とを暗号化し、｛Ｋｃ／／ＡＣ２｝Ｋｓ３をデータバスＢＳ３に出力する（ステップＳ２１７）。

【０１４４】データバスＢＳ３に出力された暗号化データは、メモリインタフェース１２００を介して携帯電話機１００に送出される。

【０１４５】携帯電話機１００においては、メモリインタフェース１２００を介してデータバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｓ３を復号処理部１２１２によって復号処理を行ない、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２を受理する（ステップＳ２１８）。復号処理部１２１２は、ライセンスキーＫｃを復号処理部１２１４に伝達し、再生回路制御情報ＡＣ２をデータバスＢＳ２に出力する。

【０１４６】コントローラ１１０６は、データバスＢＳ２を介して、再生回路制御情報ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２１９）。

【０１４７】ステップＳ２１９においては、再生回路制御情報ＡＣ２によって再生不可と判断される場合には、再生動作は終了される。

【０１４８】ステップＳ２１９において再生可能と判断された場合、コントローラ１１０６は、メモリインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、データバスＢＳ３および端子１２０１を介してメモリインタフェース１２００へ出力する（ステップＳ２２０）。

【０１４９】携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、データバスＢＳ２を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１４へ与える。そして、復号処理部１２１４は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１２から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ２２１）。

【０１５０】そして、復号されたコンテンツデータＤａｔａは音楽再生部１２１６へ出力され、音楽再生部１２１６は、コンテンツデータを再生し、ＤＡ変換器１２１８はディジタル信号をアナログ信号に変換して端子１２２０へ出力する。そして、スイッチ１２２２は端子１２２０を選択して音楽データは端子１２２４を介してヘッドホーン１３０へ出力されて再生される（ステップＳ２２２）。

【０１５１】そして、選曲されたコンテンツデータの再生動作が終了すると、更新されたメディア内曲リストＲ１に基づき再生曲リストＲ２が生成され、再表示される（Ｓ２２３）。

【０１５２】選曲（ステップＳ２０７）により複数の曲が、または同一曲が複数回選択された時には、表示動作（ステップＳ２２３）が終了する毎に、たとえば、図１４のステップＳ２０８の処理に移る。

【０１５３】このように、第１の実施の形態によれば、携帯電話機は、コンテンツデータの著作権を十分に保護しながら再生することができる。特に、ライセンスの制限を自動的に判別できるため、ユーザ側の選曲動作が簡単化される。

【０１５４】メディア内曲リストＲ１は、メモリカード１１０側に転送し、メモリカード１１０側のメモリ１４１５にも格納する。

【０１５５】なお、第１の実施の形態では、再生曲リストＲ２は、再生可能な曲データに関する情報を含むようにしたが、これに限定されない。メディア内曲リストＲ１と同様に、暗号化コンテンツデータとライセンスキーとが存在する、暗号化コンテンツデータのみが存在しライセンスキーが存在しない、ライセンスキーが存在するが暗号化コンテンツデータが存在しない、その他ライセンスによる制限に関する情報を含ませ、これらの特性を表示するようにしてもよい。

【０１５６】この場合、再生不可能な曲データが選曲されると、コントローラ１１０６は、再生処理を実行せずに、再生に必要なデータをダウンロードするか、当該曲データを削除するかをユーザに促すメッセージをディスプレイ１１１０に表示する。そして、ユーザの選択に従って、ダウンロード処理や削除を実行するようにする。これにより、ユーザによる記録データの管理が簡単化される。

【０１５７】［第２の実施の形態］第１の実施の形態では、メディア内曲リストＲ１を携帯電話機１００で生成（更新）した。これに対し、第２の実施の形態では、メモリカード１１０においてメディア内曲リストＲ１を生成する。

【０１５８】この場合、メモリカード１１０におけるコントローラ１４２０が、メモリカード１１０に格納されるデータに基づき、メディア内曲リストＲ１を生成する。メディア内曲リストＲ１は、携帯電話機１００のコントローラ１１０６の要求に応じて携帯電話機１００側に転送される。

【０１５９】そして、コントローラ１１０６は、再生モード時に、当該メディア内曲リストＲ１に基づき再生曲リストＲ２を生成し、表示する。

【０１６０】この場合であっても、第１の実施の形態と同様に、携帯電話機は、コンテンツデータの著作権を十分に保護しながら再生することができる。また、ライセンスの制限を自動的に判別できるため、ユーザ側の選曲動作が簡単化される。

【０１６１】［第３の実施の形態］第３の実施の形態による携帯電話機１００およびメモリカード１１０について説明する。携帯電話機１００およびメモリカード１１０の構成は、第１の実施の形態で説明したとおりである。

【０１６２】第３の実施の形態による携帯電話機１００は、メディア内曲リストを管理するメディア管理モードを有する。メディア内曲リストを管理するメディア管理モードについて、図１５を用いて説明する。

【０１６３】メディア内曲リストＲ１に携帯電話機１００からアクセスする前に、メモリカード１１０と携帯電話機１００との間の認証がすでになされているものとする。

【０１６４】まず、待ち受け状態にあるとする（ステップＳ３００）。ユーザによるモード指定がなされると、メディア管理モードであるか否かが判断される（ステップＳ３０２）。メディア管理モードでない場合（たとえば、上述した音楽再生モード等）は、該当する処理モードを実行する（ステップＳ３１０）。

【０１６５】メディア管理モードである場合、携帯電話機１００は、メモリカード１１０側からデータを入手する（ステップＳ３０４）。

【０１６６】そして、携帯電話機１００は、当該データに基づき、メディア内曲リストＲ１をディスプレイ１１１０に表示する（ステップＳ３０６）。表示では、特性リスト５００にある特性“Ｃ”（コンテンツデータがない）、“Ｌ”（ライセンスキーがない）、“ＬＣ”（ライセンスによる制限があり、制限を超えた）、コンテンツデータとライセンスキーとが存在する等をユーザが認識できるように表示する。なお、色による区別をつけてもよい。

【０１６７】表示内容は、これに限定されず、特性“Ｃ”（ライセンスのみの曲）、“Ｌ”（コンテンツのみの曲）、“ＬＣ”（再生の回数制限を越えた曲）、“ＬＮ”（再生の時間制限を越えた曲）の他にライセンス制限がある曲の表示マークがあってもよい。

【０１６８】そして、メディア内曲リストＲ１のデータ編集を行う（ステップＳ３０８）。編集処理において、ライセンスまたは／およびコンテンツデータの削除、再生番号の順番の変更が可能となる。編集の途中経過、および結果は、すべてディスプレイ１１１０に表示される。

【０１６９】なお、各曲データに個人的な情報付加することも可能である。ただし、ライセンスキーやコンテンツデータの改ざんはできない。

【０１７０】編集後、メディア内曲リストＲ１をメモリカード１１０に転送する。このように、第３の実施の形態によれば、コンテンツに関連するデータをユーザ側で編集することができるため、ユーザ側の意向にそったデータ管理が可能になる。

【０１７１】［第４の実施の形態］第３の実施の形態では、メディア内曲リストＲ１を携帯電話機１００で生成し、編集する場合について説明した。これに対し、第４の実施の形態では、メモリカード１１０でメディア内曲リストＲ１を生成し、携帯電話機１００で編集する場合について説明する。

【０１７２】この場合、携帯電話機１００は、メディア管理モードになると、図１５に示すステップＳ３０４の代わりに、メモリカード１１０からメディア内曲リストＲ１を読出す処理を行う。そして、メモリカード１１０から受取ったメディア内曲リストＲ１をステップＳ３０６で表示する。

【０１７３】そして、ステップＳ３０８において、メディア内曲リストＲ１のデータ編集を行う。編集処理においては、たとえば、再生番号の順番の変更が可能となる。編集の途中経過、および結果は、すべてディスプレイ１１１０に表示される。

【０１７４】編集後、メディア内曲リストＲ１をメモリカード１１０に転送する。このように、第４の実施の形態によれば、コンテンツに関連するデータをユーザ側で編集することができるため、ユーザ側の意向にそったデータ管理が可能になる。

【０１７５】［第５の実施の形態］第１の実施の形態では、メディア内曲リストＲ１の更新に基づき、再生曲リストＲ２を更新した。これに対し、第５の実施の形態では、音楽再生モード中は、再生曲リストＲ２を直接ライセンスの制限に従って更新する。

【０１７６】このため、第５の実施の形態では、音楽再生モードが開始されると、携帯電話機は、携帯電話機内においてアクセスに関する情報を管理する。たとえば、第１の実施の形態による構成では、携帯電話機１００側にアクセスに関する情報（アクセス制限情報ＡＣ１）を転送する。転送後、携帯電話機は、携帯電話機１００内においてアクセスに関する情報を管理する。携帯電話機で管理するアクセスに関する情報を、再生回数に関する情報ＡＣＫ１と称す。

【０１７７】なお、暗号・復号方式、認証方式は第１の実施の形態によるものには限定されない。再生側として携帯電話機（たとえば、携帯電話機１００）を、メディア側としてメモリカード（たとえば、メモリカード１１０）を代表例として説明する。以下の説明では、メモリカード側における携帯電話機に対する認証は正当であるものとする。

【０１７８】第５の実施の形態による音楽再生モードでの処理の概要について、図１６を用いて説明する。まず、待ち受け状態にある（ステップＳ４００）。指示に従いモード判定を行う（ステップＳ４０２）。なお、音楽再生モードであると判定されると、メディア内曲リストＲ１に基づき、再生曲リストＲ２が生成され、ディスプレイ１１１０に表示される（ステップＳ４０４）。

【０１７９】音楽再生要求（選曲）があるか否かが判定される（ステップＳ４０６）。再生要求がない場合には、ステップＳ４０４に移る。

【０１８０】音楽再生要求があると、選曲された曲データが、ライセンスにより再生回数に制限があるか否かが判定される（ステップＳ４０８）。制限がなければ、暗号化コンテンツデータを所定の形式で復号化して、音楽を再生する（ステップＳ４２２）。そして、音楽終了要求があるか否かが判定され（ステップＳ４２４）、終了要求があればステップＳ４０４へ、終了要求が無ければステップＳ４２２の再生状態を継続する。

【０１８１】ライセンスにより再生回数に制限のある曲を再生する場合には、再生回数が限度に達したか否かが判断される（ステップＳ４１０）。再生回数が最終でない場合には、再生回数に関する情報ＡＣＫ１を更新する（ステップＳ４２０）。そして、ステップＳ４２２の処理に移る。

【０１８２】再生回数が最後の再生であった場合には、音楽を再生する処理（ステップＳ４１２）に移る。そして、音楽終了要求があるか否かが判定され（ステップＳ４１４）、終了要求があればステップＳ４１６へ、終了要求が無ければステップＳ４１２の再生状態を継続す

る。

【0183】再生回数が最後の再生後に音楽終了要求があると、再生曲リストR2から再生した曲データを削除し、再生曲リストR2を再構築する（ステップS416）。これにより、再生可能な曲データのリストと、対応する再生番号が修正される。

【0184】そして、曲を再生する度にメディア内曲リストR1を更新し、対応する曲データについて、ライセンスにより再生できない旨を示すマーク（たとえば、“LC”）をつける（ステップS418）。

【0185】音楽再生モードが終了すると、メディア内曲リストR1は、メモリカード110に転送される。

【0186】このように、第5の実施の形態では、音楽再生モードに入ると、携帯端末側（再生系側）で、ライセンスによる制限に基づき再生曲リストR2が自動的に更新される。

【0187】これにより、第1の実施の形態と同様、ライセンスの制限を自動的に判別できるため、ユーザ側の選曲動作が簡単化される。

【0188】なお、上記説明では再生回数のみに限定して説明したが、ライセンスにより制限のあるものであればいずれにも適用される。

【0189】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

【図5】 ライセンスサーバの構成を示す概略ブロック図である。

【図6】 携帯電話機の構成を示すブロック図である。

【図7】 メモリカードの構成を示すブロック図である。

【図8】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図9】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図10】 （a）メディア内曲リストR1、（b）再生曲リストR2をそれぞれ示す概念図である。

【図11】 （a），（b）は、メディア内曲リストR1の更新状況を説明するための概念図である。

【図12】 （a），（b），（c）は、再生曲リストR2の更新状況を説明するための概念図である。

【図13】 携帯電話機における再生動作を説明するための第1のフローチャートである。

【図14】 携帯電話機における再生動作を説明するための第2のフローチャートである。

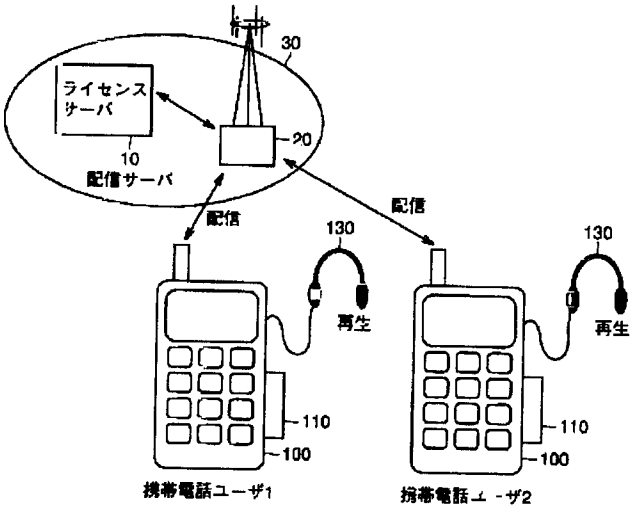
【図15】 携帯電話機におけるメディア管理モードでの処理内容を説明するためのフローチャートである。

【図16】 第5の実施の形態による音楽再生モードでの処理動作を説明するためのフローチャートである。

【符号の説明】

10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、100携帯電話機、110 メモリカード、130 ヘッドホーン、140 コンピュータ、141 ハードディスク、142，1106，1420 コントローラ、143 外部インタフェース、144 ライセンス保護モジュール、145 通信ケーブル、302 課金データベース、304 情報データベース、306CRLデータベース、310 データ処理部、312，320，1206，1212，1214，1404，1408，1412，1422 復号処理部、315 配信制御部、316，1210，1418 セッションキー発生部、318，326，328，1208，1410 暗号化処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108，1224 キー操作部、1110 ディスプレイ、1112 音声再生部、1113，1218 DA変換器、1114，1201，1220，1224 端子、1200 メモリインタフェース、1222 スイッチ、1402 Kmc1保持部、1414，1414B KPma保持部、1415 メモリ、1416 KPm1保持部、1421 Km1保持部、1440 ライセンス情報保持部、1442，1444，1446 切換スイッチ、1202，1400 認証データ保持部、1204 Kp1保持部、1216 音楽再生部。

【図1】



【図2】

名称	属性	保持/発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可）
AC	ライセンス購入条件		利用者側から指定(例：ライセンス改,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報（例：再生可否）

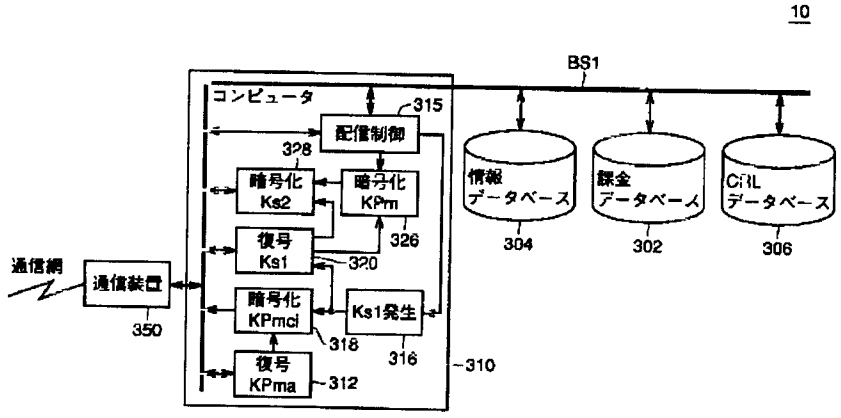
【図3】

名称	属性	保持/発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報（差分データ形式）
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
$KP_{\mu n}$	公開暗号鍵（非対称鍵）	携帯電話機	Kpnにて復号可能。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機の種類nごとに異なる。
KPmci	公開暗号鍵（非対称鍵）	メモリカード	Kmciにて復号可能。 {KPmci//Cmci}KPmaの形式で出荷時に記録 ＊メモリカードの種類ごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 ＊携帯電話機の種類nごとに異なる。
Kmci	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ＊メモリカードの種類ごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機のクラスnごとに異なる。
Cmci		メモリカード	メモリカードのクラス証明書。認証機能を有する。 {KPmci//Cmci}KPmaの形式で出荷時に記録 ＊メモリカードのクラスごとに異なる。

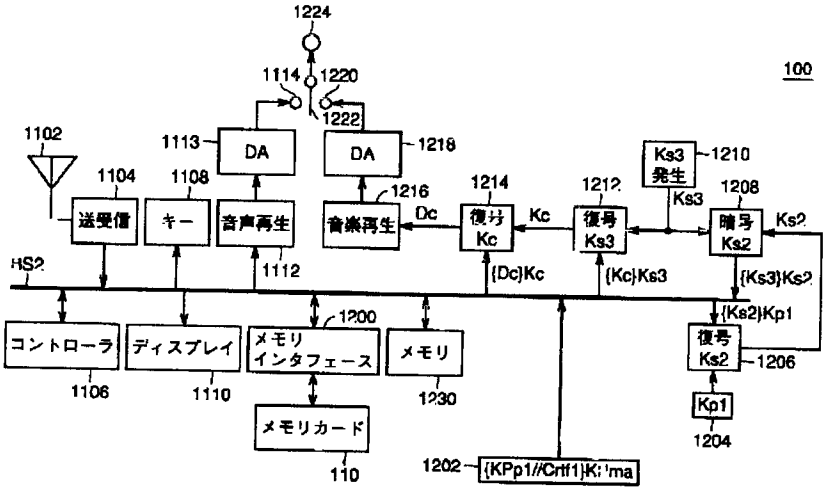
【図4】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 （非対称鍵）	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

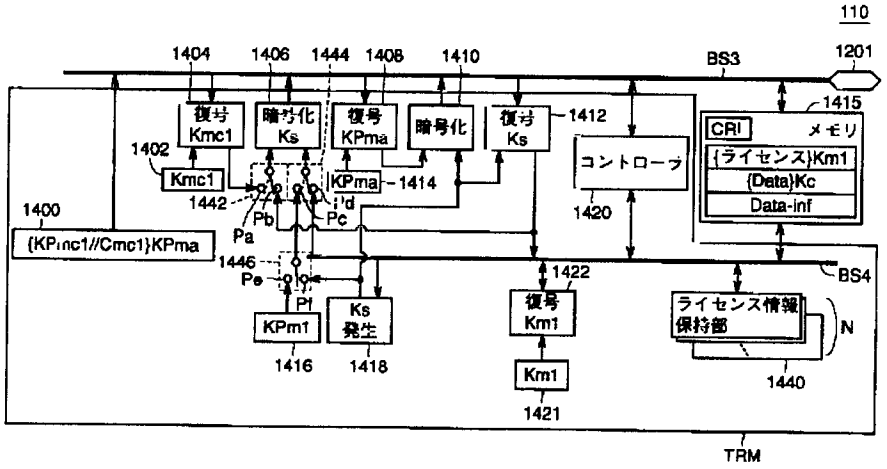
【図5】



【図6】

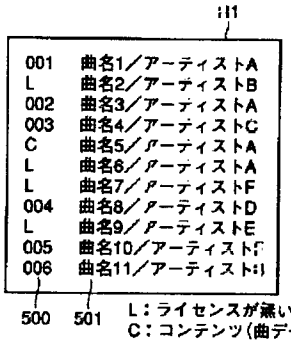


【図7】



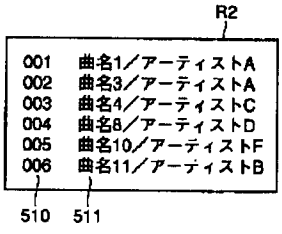
【図10】

(a) メディア内曲リスト



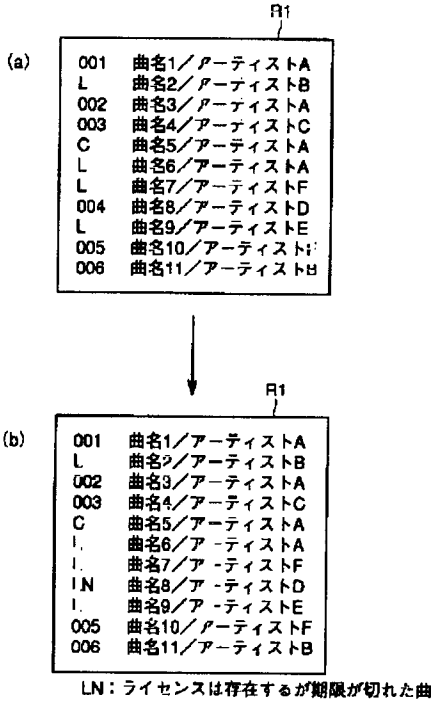
L：ライセンスが無い曲
C：コンテンツ（曲データ）が無い曲

(b) 再生曲リスト



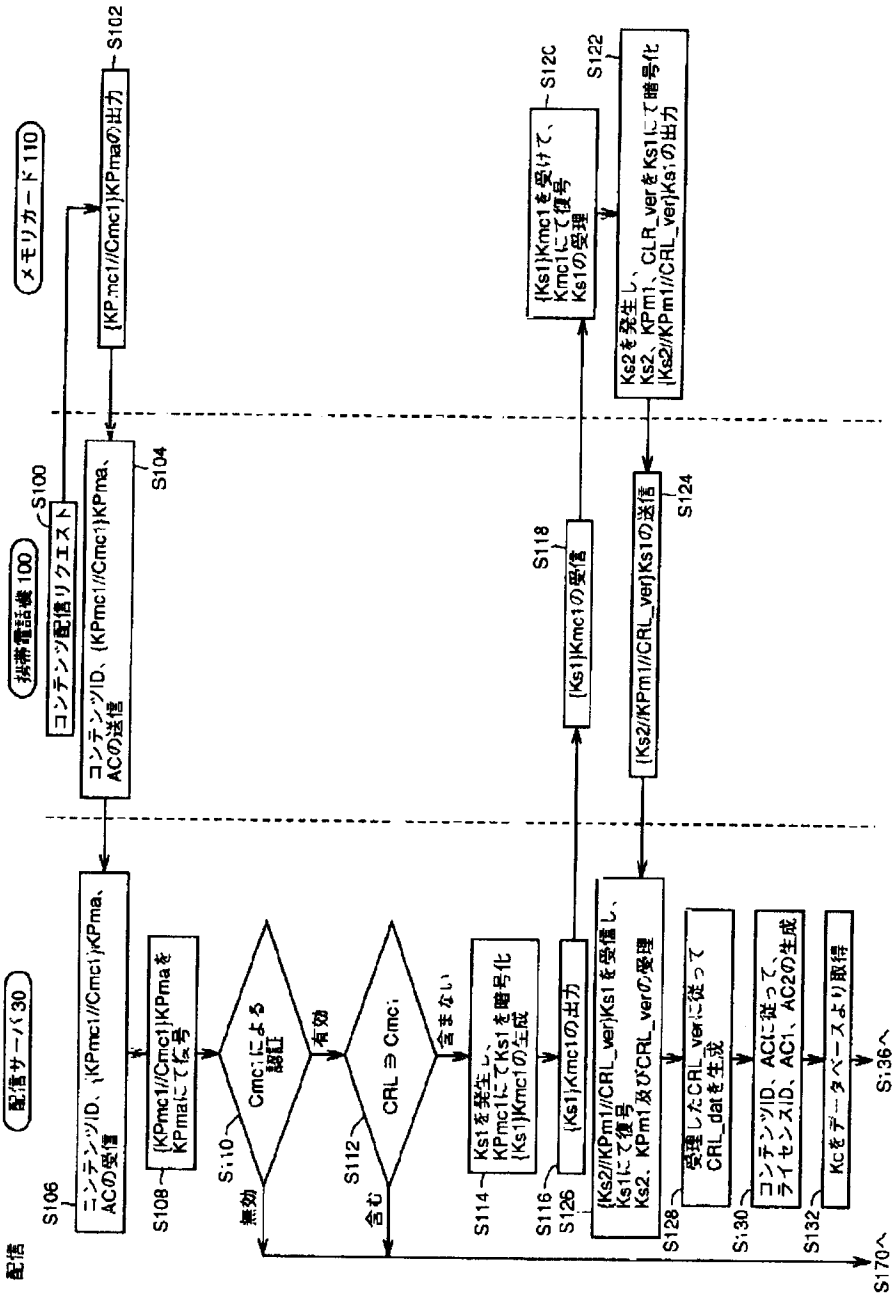
【図11】

メディア内曲リスト

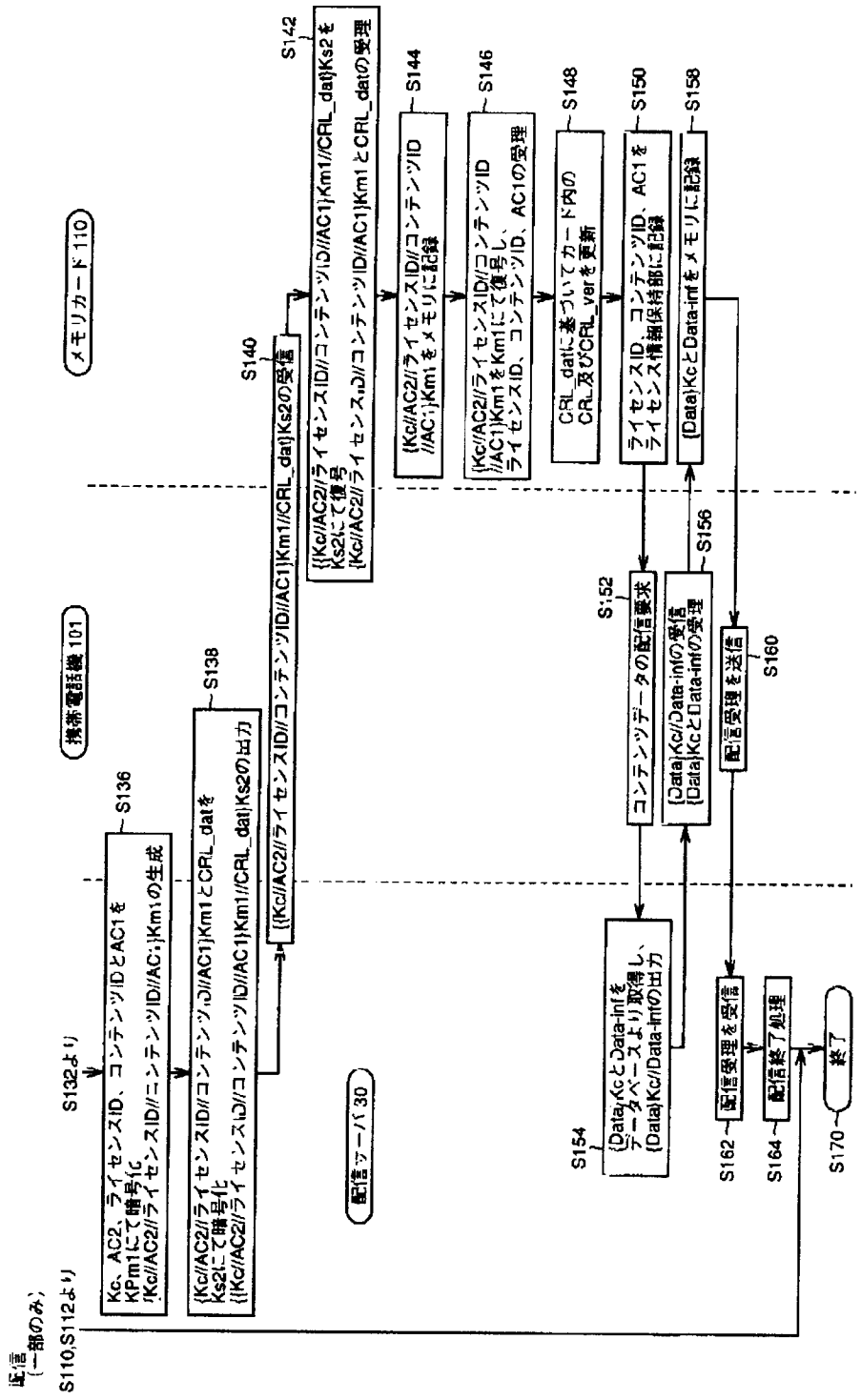


LN：ライセンスは存在するが期限が切れた曲

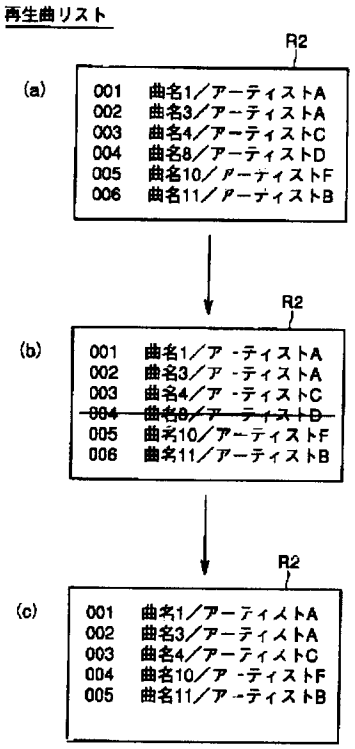
【図8】


メモリカード110
携帯電話機100
配信サーバ30
配信
S100
コンテンツ配信リクエスト
S102
{KPmc1//Cmc1}KPmaの出力
コンテンツID、{KPmc1//Cmc1}KPma、ACの送信
S104
S106
コンテンツID、{KPmc1//Cmc1}KPma、ACの受信
S108
{KPmc1//Cmc1}KPmaをKPmaにて復号
S110
Cmciによる認証
無効
有効
S112
CRL ∋ Cmci
含む
含まない
S114
Ks1を発生し、KPmc1にて{Ks1}Kmc1の生成
S116
{Ks1}Kmc1の出力
S118
{Ks1}Kmc1の受信
S120
{Ks1}Kmc1を受けて、Kmc1にて復号
Ks1の受理
S122
Ks2を発生し、Ks2、KPm1、CLR_verをKs1にて暗号化{Ks2//KPm1//CRL_ver}Ksiの出力
S124
{Ks2//KPm1//CRL_ver}Ks1の送信
S126
{Ks2//KPm1//CRL_ver}Ks1を受信し、Ks1にて復号
Ks2、KPm1及びCRL_verの受理
S128
受理したCRL_verに従ってCRL_datを生成
S130
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S132
Kcをデータベースより取得
S136へ
S170へ

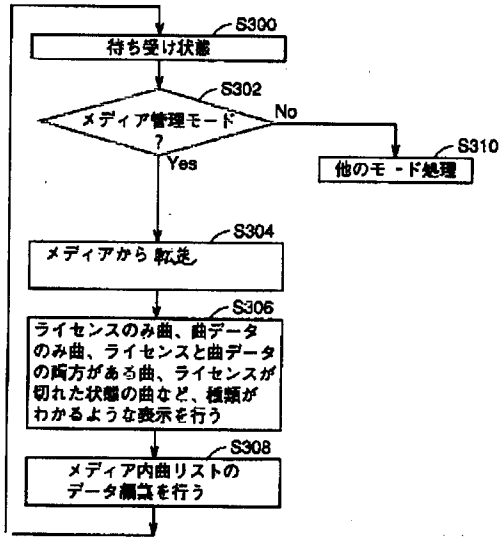
【図9】


メモリカード 110
携帯電話機 101
配信サーバ 30
S110,S112より
(一部のみ)
S132より
S136
Kc、AC2、ライセンスID、コンテンツIDとAC1を
KPm1にて暗号化
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1の生成
S138
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の出力
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受信
S140
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datの受理
S142
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をメモリに記録
S144
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km1をKm1にて復号し、
ライセンスID、コンテンツID、AC1の受理
S146
CRL_datに基づいてカード内の
CRL_及びCRL_verを更新
S148
ライセンスID、コンテンツID、AC1を
ライセンス情報保持部に記録
S150
{Data}Kcと{Data}Data-infをメモリに記録
S158
S152
コンテンツデータの配信要求
S154
{Data}Kcと{Data}Data-infを
データベースより取得し、
{Data}Kc//Data-infの出力
{Data}Kc//Data-infの受信
{Data}Kcと{Data}Data-infの受理
S156
配信受理を送信
S160
配信受理を受信
S162
配信終了処理
S164
終了
S170

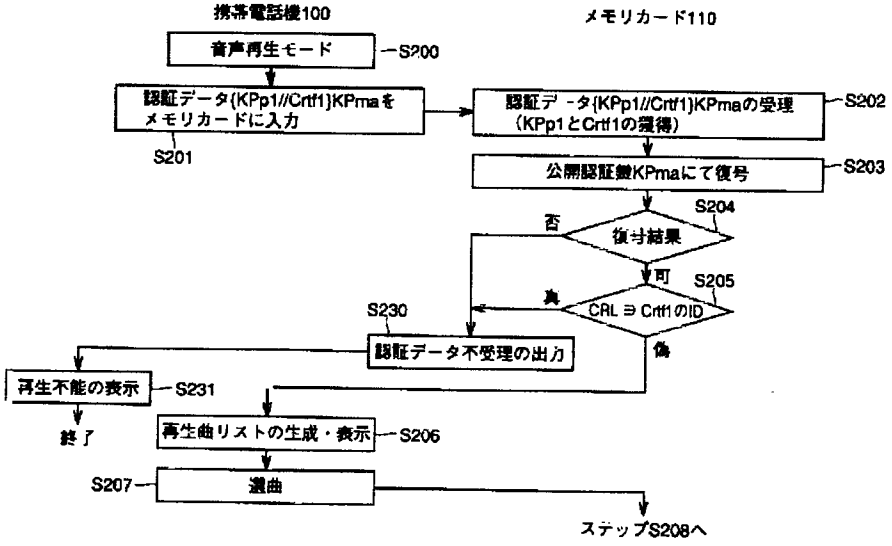
【図12】


再生曲リスト
R2
(a)
001 曲名1／アーティストA
002 曲名3／アーティストA
003 曲名4／アーティストC
004 曲名8／アーティストD
005 曲名10／アーティストF
006 曲名11／アーティストB
R2
(b)
001 曲名1／アーティストA
002 曲名3／アーティストA
003 曲名4／アーティストC
004 曲名8／アーティストD
005 曲名10／アーティストF
006 曲名11／アーティストB
R2
(c)
001 曲名1／アーティストA
002 曲名3／アーティストA
003 曲名4／アーティストC
004 曲名10／アーティストF
005 曲名11／アーティストB

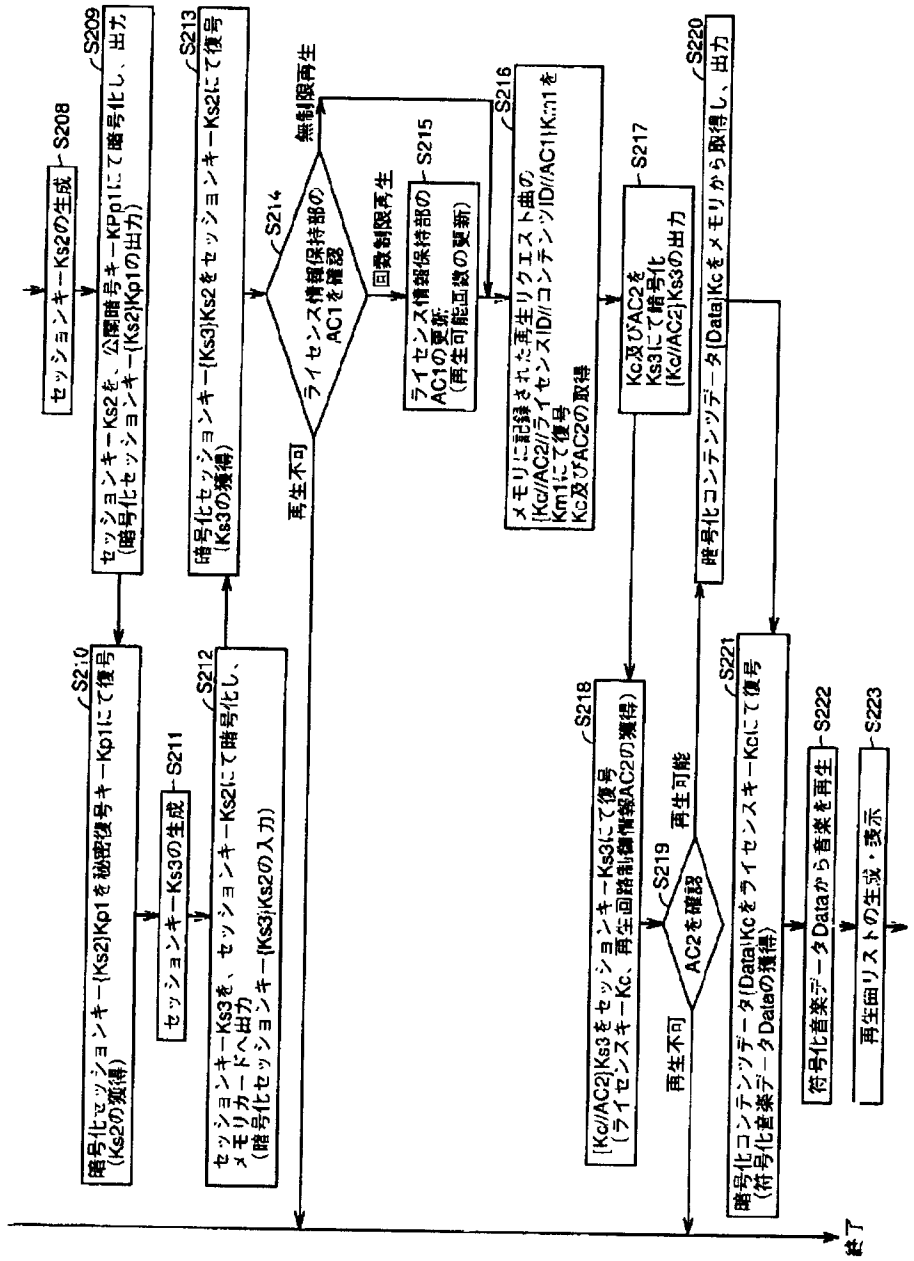
【図15】


S300
待ち受け状態
S302
メディア管理モード？
No
Yes
S310
他のモード処理
S304
メディアから転送
S306
ライセンスのみ曲、曲データのみ曲、ライセンスと曲データの両方がある曲、ライセンスが切れた状態の曲など、種類がわかるような表示を行う
S308
メディア内曲リストのデータ編集を行う

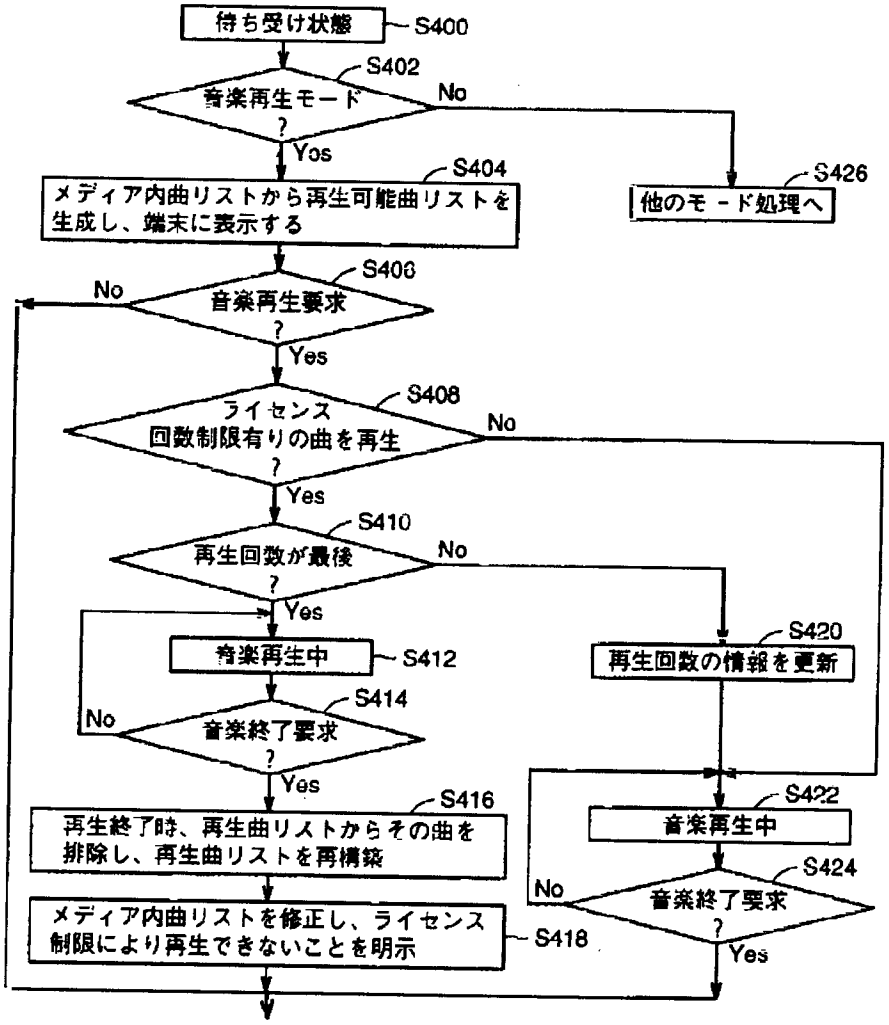
【図13】


携帯電話機100
メモリカード110
音声再生モード
S200
認証データ{KPp1//Crtf1}KPmaをメモリカードに入力
S201
認証データ{KPp1//Crtf1}KPmaの受理（KPp1とCrtf1の獲得）
S202
公開認証鍵KPmaにて復号
S203
S204
復号結果
否
可
S205
真
CRL ∋ Crtf1のID
偽
S230
認証データ不受理の出力
再生不能の表示
S231
終了
再生曲リストの生成・表示
S206
S207
選曲
ステップS208へ

【図14】


セッションキーKs2の生成
S208
セッションキーKs2を、公開暗号キーKPp1にて暗号化し、出力
(暗号化セッションキー{Ks2}Kp1の出力)
S209
暗号化セッションキー{Ks2}Kp1を秘密復号キーKp1にて復号
(Ks2の獲得)
S210
セッションキーKs3の生成
S211
セッションキーKs3を、セッションキーKs2にて暗号化し、
メモリカードへ出力
(暗号化セッションキー{Ks3}Ks2の入力)
S212
暗号化セッションキー{Ks3}Ks2をセッションキーKs2にて復号
(Ks3の獲得)
S213
ライセンス情報保持部のAC1を確認
S214
無制限再生
再生不可
回数制限再生
ライセンス情報保持部のAC1の更新
(再生可能回数の更新)
S215
メモリに記録された再生リクエスト曲の
{Kc//AC2}//ライセンスID//コンテンツID//AC1{Km1}を
Km1にて復号
Kc及びAC2の取得
S216
Kc及びAC2を
Ks3にて暗号化
{Kc//AC2}Ks3の出力
S217
暗号化コンテンツデータ{Data}Kcをメモリから取得し、出力
S220
{Kc//AC2}Ks3をセッションキーKs3にて復号
(ライセンスキーKc、再生回路制御情報AC2の獲得)
S218
AC2を確認
S219
再生可能
再生不可
暗号化コンテンツデータ{Data}Kcをライセンスキー{Kc}にて復号
(符号化音楽データDataの獲得)
S221
符号化音楽データDataから音楽を再生
S222
再生曲リストの生成・表示
S223
終了

【図16】


待ち受け状態
S400
S402
音楽再生モード
?
No
Yes
S404
メディア内曲リストから再生可能曲リストを
生成し、端末に表示する
S426
他のモード処理へ
S406
音楽再生要求
?
No
Yes
S408
ライセンス
回数制限有りの曲を再生
?
No
Yes
S410
再生回数が最後
?
No
Yes
音楽再生中
S412
S420
再生回数の情報を更新
S414
音楽終了要求
?
No
Yes
S416
再生終了時、再生曲リストからその曲を
排除し、再生曲リストを再構築
S422
音楽再生中
S424
音楽終了要求
?
No
Yes
メディア内曲リストを修正し、ライセンス
制限により再生できないことを明示
S418